WATERMARK SYSTEMS FOR MEDIA

Related Application Data

This application claims priority to provisional application 60/257,822, filed December 21, 2000.

Field of the Invention

The present disclosure memorializes various improvements relating to digital watermarking technology and applications.

Background of the Invention

Digital watermarking is the science of encoding physical and electronic objects with plural-bit digital data, in such a manner that the data is essentially hidden from human perception, yet can be recovered by computer analysis. In physical objects, the data may be encoded in the form of surface texturing, or printing. Such marking can be detected from optical scan data, e.g., from a scanner or web cam. In electronic objects (e.g., digital audio or imagery – including video), the data may be encoded as slight variations in sample values. Or, if the object is represented in a so-called orthogonal domain (also termed "non-perceptual," e.g., MPEG, DCT, wavelet, etc.), the data may be encoded as slight variations in quantization values or levels. The present assignee's patent 6,122,403, and application 09/503,881, are illustrative of certain watermarking technologies.

Watermarking can be used to tag objects with a persistent digital identifier, and as such finds myriad uses. Some are in the realm of device control – e.g., tagging video data with a do-not-copy flag that is respected by compliant video recorders. (The music industry's Secure Digital Music Initiative (SDMI), and the motion picture industry's Copy Protection Technical Working Group (CPTWG), are working to establish standards relating to watermark usage for device control.) Other watermark applications are in the field of copyright communication, e.g., indicating that an audio track is the property of a particular copyright holder.

Other watermark applications encode data that serves to associate an object with a store of related data. For example, an image watermark may contain an index value that serves to identify a database record specifying (a) the owner's name; (b) contact information; (c) license terms and conditions, (d) copyright date, (e) whether adult content is depicted, etc., etc. (The present assignee's MarcCentre service provides such functionality.) Related are so-called "connected content" applications, in which a watermark in one content object (e.g., a printed magazine article) serves to link to a related content object (e.g., a web page devoted to the same topic). The watermark can literally encode an electronic address of the related content object, but more typically encodes an index value that identifies a database record containing that address information. Application 09/571,422 details a number of connected-content applications and techniques.

One problem that arises in many watermarking applications is that of object corruption. If the object is reproduced, or distorted, in some manner such that the content presented for watermark decoding is not identical to the object as originally watermarked, then the decoding process may be unable to recognize and decode the watermark. To deal with such problems, the watermark can convey a reference signal. The reference signal is of such a character as to permit its detection even in the presence of relatively severe distortion. Once found, the attributes of the distorted reference signal can be used to quantify the content's distortion. Watermark decoding can then proceed – informed by information about the particular distortion present.

The assignee's applications 09/503,881and 09/452,023 detail certain reference signals, and processing methods, that permit such watermark decoding even in the presence of distortion. In some image watermarking embodiments, the reference signal comprises a constellation of quasi-impulse functions in the Fourier magnitude domain, each with pseudorandom phase. To detect and quantify the distortion, the watermark decoder converts the watermarked image to the Fourier magnitude domain and then performs a log polar resampling of the Fourier magnitude image. A generalized matched filter correlates the known orientation signal with the re-sampled watermarked signal to find the rotation and scale parameters providing the highest correlation. The

watermark decoder performs additional correlation operations between the phase information of the known orientation signal and the watermarked signal to determine translation parameters, which identify the origin of the watermark message signal. Having determined the rotation, scale and translation of the watermark signal, the reader then adjusts the image data to compensate for this distortion, and extracts the watermark message signal as described above.

With the foregoing by way of background, the specification next turns to the various improvements. It will be recognized that these improvements can typically be employed in many applications, and in various combinations with the subject matter of the patent documents cited herein.

DETAILED DESCRIPTION

Watermarks in Video and Broadcast Programming

Several novel uses of watermarks relate to video and broadcast programming. For example, a watermark may be placed at a certain location in content (e.g., audio or video), and serve to trigger insertion or play of an advertisement. Conditional rules can be specified (e.g., play advertisement X if the current hour is between 9:00 p.m. and 5:00 a.m.; play advertisement Y if the current hour is between 5:00 a.m. and 9:00 p.m.).

Another is to charge differently for content, depending on whether or not it is rendered with advertisements included. For example, if a viewer fast-forwards through advertising in a video program, then a charge is assessed for the viewing. Else no charge (or a reduced charge) is assessed. (A related concept is disclosed in application 09/337,590, filed 6/21/99.)

Watermarks (e.g., watermark advertising triggers) may be counted by a system and, when a threshold of number or types of watermarks detected is reached, playback of specific advertising or other material is completed. Thus, if a viewer has apparently watched five advertisements, no more advertisements are inserted for a predetermined period (or through the end of the current content). Or if the viewer has watched two automobile ads (or two Ford ads), no further automobile ads will be presented. (Conversely, the viewer's willingness to watch automobile ads may indicate that such

ads should be inserted in preference to another class of ads over which the viewer habitually fast-forwards or otherwise does not view, e.g., for financial service institutions.) In addition, the watermark may have a date-time stamp, or time counter that can help determine how long the content has been playing. For example, the user may have started viewing at 2000 seconds, and at 2600 seconds, or 10 minutes of viewing, an advertisement is triggered.

A variation of this concept involves personalized advertisement delivery triggered by watermarks. For example, advertisements tailored to particular consumer profiles (e.g., based on zip codes or other known general or specific demographic information) may be downloaded to a Tivo-like Personal Video Recorder (PVR) through known video sources (e.g., a set top box, coupled to cable, satellite, etc.). These tailored advertisements can be inserted based upon detection of specific watermark triggers (e.g., akin to how local advertising is inserted in national network programming). Or generic advertising already included in the content can be watermarked and, if a tailored advertisement is locally stored and has a corresponding watermark, it can be substituted for the generic advertisement. Or after three generic advertisements, a personalized advertisement may be inserted. Many other such variations are naturally possible.

Instead of caching tailored advertising in a Tivo-like device, such advertising can be distributed otherwise. One example is a DVD video disk mailed to the consumer. Playback of advertising from this disk can be triggered by watermark signals in other content, and – as above – can benefit the consumer by reduced cost- or free-viewing of otherwise premium content.

Instead of substituting locally-stored advertising in externally received content, the opposite arrangement can be employed. A DVD video, a PVR replay, etc., can be periodically interrupted (based on watermark trigger signals), and advertising from another source (e.g., cable, wireless, etc.) may be inserted.

The advertising can be tailored to the viewer, or can be tailored to the programming. Thus, for example, programming showing a golf tournament may be so-indicated by a watermark, and this watermark can thereby signal that golf-related

advertising should be inserted. (The watermark may convey an index value that is associated – through a remote data store – with the programming subject, or the watermark may literally convey a code corresponding to the programming subject.)

Playback of advertising may enable access to other content or capabilities. This can occur by requiring a number or type of watermark to be read (e.g., beginning/middle/end) before viewing of other content is permitted (akin to requiring theatre-goers to watch trailers for upcoming movies before viewing the featured movie). Once the watermarks are detected from the requisite advertisements, then the viewer is permitted to access additional content, or exercise other capabilities.

A secondary watermark (in addition to a primary content owner or creator watermark) can be employed to enable broadcasters, cable operators, content aggregators, etc., to add connected content functionality – directing users back to pre-arranged web sites, etc. (e.g., a web site maintained by the broadcaster, aggregator, etc.). Such functionality may be in addition to the simultaneous linking capabilities available to the content owner/creator's web site). Set top boxes, DVD/CD players or other devices can be able to detect both types of watermarks, and route users to either class of destination based on pre determined rules or customer preference.

Connected Content and Peer-to-Peer Sharing

It is not clear that Napster-like sharing of movies will be as popular as such sharing of audio. Regardless, it seems watermarking can play an important role.

Unlike audio, most people are not accustomed to "owning" a movie. Instead, rental or PPV is the dominant user experience.

One particular approach is to provide the content data for free, and assess a charge for its playback (rendering). The charge can be triggered upon detection of a watermark.

A watermark can also be used for connected-content purposes. One such application permits the user to obtain (e.g., download) movies and songs that are mentioned, or relate to, the video content being viewed. The watermark can be conveyed in the audio track, and/or the video content (or each could include one or

more different marks). In one scenario, a device like that disclosed in application 09/476,686 (filed December 30, 1999) is used to listen to ambient sound, and decode any watermark in such sound. When a watermark is detected indicating, e.g., that the viewer is watching the movie Mission Impossible, the device and related software can search for related content. This can be accomplished, e.g., by using an index value conveyed by the watermark to access a store of meta data associated with the movie. That store can contain the title of the movie, titles of pre-quels, sequels, names of stars, name of the movie director, geographic locations featured, featured music, etc. A catalog of available audio and/or video can then be searched in accordance with such meta data to identify related content. The results of the search can be presented to the viewer, who can choose one or more for linking. Alternatively, instead of searching based on keywords, a data store associated with the watermark index value can directly identify related content, e.g., by title and web address. Again, this information can be presented to the user for futher linking. A great variety of other such arrangements are naturally possible.

In some such arrangements, the connected content does not have a sole, known source. Instead, it may be located in a peer-to-peer media sharing service, akin to Napster, and downloaded from whatever source the user – or some computer-executed procedure – dictates.

Likewise, the original source video may be obtained by the user from a peer-to-peer network (e.g., like a video-Napster). Again, the content may be obtained for free, and a charge levied only when the content is viewed. This charge can be triggered by watermark detection, or using various non-watermark techniques. The charge may be fixed, but can alternatively be on a per-increment of viewing (e.g., a nickel charged for every 5 minutes rendered to the user). Still further, the content can be provided in streaming form, rather than as one or more discrete files.

In this and many content delivery systems, streaming can be used as an alternative to file transfer when the recipient's rights to have a file copy of the content cannot be confirmed.

The advantage of a peer-to-peer architecture is that a massive central server needn't serve the requests of all possible users. Instead, this function is spread over a widely distributed network, providing consumers with a service that is faster and – potentially – less expensive.

Connected Content and Advertising

Another concept is to include connected-ads within (as opposed to interrupting) the entertainment. If someone "clicks" on (or during) the ad, or otherwise activates same, then they receive money towards watching the TV show. If someone doesn't want to click on the ad, they pay for the show. The ads are linked to information via watermarks.

For example, if Ross in the TV show Friends is drinking a Coke during the show, then clicking during that time will present the viewer with linking options, one of which is viewing the web page of Coke. It will be identified that this is an advertising link, possibly with an ad credit symbol such as a $. If the user clicks on this option, they will receive some benefit, such as x cents deducted from their monthly TV bill. Thus, if they want to watch TV without ads, they just don't click on ads and pay more for the monthly TV bill.

Alternatively, the user could click on the ad link and bookmark it for usage at a later time, at which time the user would receive their credit. In addition, if different video objects are marked with different watermarks, then clicking on the Coke can can take the user directly to the ad page, or bookmark same for future use.

One advantage of this approach over traditional ad models is that the consumer can decide how much advertising to watch and pay accordingly, while watching the same show as other consumers who want advertising. In other words, you don't need different shows and channels, such as a premium show and related channel and a free show and related channel.

While watermarks are preferred in this application to convey data related to the connected content (e.g., advertising), other known data transmission mechanisms can

be used (e.g., Multicast IP, vertical blanking interval-based systems, file headers in MPEG, etc.).

Different on-screen signals (icons, etc.) can be used to indicate to the viewer that advertising / information / money saving opportunities exist for the viewer, and that the viewer can earn credits towards purchasing merchandise by watching the ad or viewing more information (akin to GreenStamps for those old enough to remember them). To continue the Coke idea, clicking on the Coke can on the TV could print a coupon for $.50 off a 6 pack of Coke at 7 Eleven.

Watermarks in Media Customization and Control; Age-Based Systems

Another application of watermark is in tailoring audio or video content presented to consumers, e.g., withholding adult materials from juvenile audiences.

A rating field, such as two bits (X, R, PG, and G), can be included in the watermark payload and identify the rating of the corresponding content on a per-video-frame (or per-audio-excerpt). The watermark reader (optionally using read-ahead capabilities) can cause the rendering device to act appropriately for non-appropriate content, such as removing adult rated-X frames. If the watermark also contains a unique ID, a secondary database can be consulted to determine the network location of alternate frames/excerpts that can then be substituted for the objectionable content. If no ID is present, default filler material can be substituted, either from a remote source, or from the consumer's own data stores (e.g., a TiVo device).

Detection of the adult content watermark bit(s) can be performed by the consumer device, or upstream in the content distribution network (e.g., in a hub, firewall, router, server, operating system, etc.) Many corporations will want the firewall to detect the adult content so that employees don't waste company time and money on viewing inappropriate materials. In addition, viewing adult content, such as pornography or violent scenes, can produce internal human resource legal problems for corporations.

While adult content is one class of content, the use of watermarks to categorize content, e.g., for filtering purposes, finds other applications as well. One is indexing.

Content can be watermarked with data indicating content classification (or with an ID that permits its content to be ascertained by checking a corresponding database record). Search engines can then index content based during web crawling.

The concept is that the watermark categorizes the content. Systems then use the watermark to make content specific decisions, like sorting, indexing, controlling playback, etc. The systems can be filters at various stages- operating system, driver, application, firewall, router, etc. The systems can be search engines or crawlers, etc.

In systems like Digimarc's Image Commerce system, in which content providers pay an annual fee so they can watermark a unique identifier into their content (which identifier permits customers to link back to the content's source), the fee can be waived for adult content. Instead of including a unique ID, the watermark payload can include a default ID. If customers link using the default ID, they are routed to a default page shared by all, e.g., adult content providers. The advantage, of course, is that a financial cost associated with watermarking is waived for such content, hopefully assisting in the ubiquitous "adult" marking of objectionable content.

(Related disclosure can be found in applications 09/636,102 and 09/706,505.)

Identification documents, such as drivers' licenses, credit cards, and other identity tokens, can include a watermark that encodes – or otherwise represents – the holder's birthdate. By displaying the document to a web camera and associated application, the birthdate can be decoded and used to authorize viewing, e.g., of R-rated content. This card can also be used to confirm a user's age for online gambling. In addition, the birthdate can allow a user to obtain pornography and gambling, anonymously while enabling the site owner to not have to worry about under age participants.

The birth date can also include an ID that can be used to identify the person needs to be identified, such as for online voting or access to restricted information on the web.

The card could be something mailed to the person after verifying their birth date, and identification if a user ID is included. The card could even be emailed and printed by the end user, although copying such a card will be easier.

Finally, the card may save the birth date via other methods, such as on a magenetic strip or through smart card chip technology, or with a combination of technologies, including watermark. The card may also contain a frail watermark such that a duplicate can be detected.

Watermarks and Media Distribution

The following section details particular watermark-related actions that can be utilized when distributing digital content.

1. Identify (ID) content with watermark

2. Use watermarked ID to trigger automated purchase and file transfer operation from source to user's machine, digital locker, etc. (e.g., press button while listening to song to trigger transaction), may include some notions of digital money transaction (see, e.g., , application 09/337,590)

3. Embed ID in an automated fashion on users' machines: search for content on drive, look up ID from local or network database (with either fingerprint or TOC type indicators), embed ID into content

4. Embed ID at time of rip, where the file transfer "client" (which acts as both client and server) includes read/write functionality. The write function can be used for supplementing previous embedding by content owner or ripper software (see, e.g., applications 09/563,664 and 09/578,551). During download, adding the unique ID from a fingerprint and secondary second database .

5. Check file for proper naming, labeling before adding to file sharing registry of content items (songs)

6. Update a listing of name - ID mapping, increment registry in real time

7. Mark file with user's ID during a download, then if user attempts to add to a file sharing system, the system knows the user and informs them how the user can and cannot use the file; e.g., refuse registration

8. Distinguish level of service in subscription service by watermark label (see, e.g., application 09/620,019)

9. check integrity of file: free of content bombs and viruses (see, e.g., application 09/620,019)

10. Use date-time stamp to control changing of rights over time (see, e.g., application 60/232,163). The date time stamp can be referenced to January 1, 2000 and incremented from there, possibly in seconds or minutes.

11. During transfer of a content object (e.g., by streaming or file transfer), a fingerprint or meta-tag obtained from the object can be parsed from the in-transfer object and used as an ID to access a database record. The database record can contain pre-existing information that can be read by the client device (e.g., to ascertain permitted usage rights). Or the database record can be written, e.g., with the date, time, username, etc., relating to the transfer.

12. Audio excerpts (e.g., individual MP3 frames) can be hashed (e.g., yielding 16 bits). This hash code can be used to modulate bits – making it more difficult to change the audio.

13. Different beginning and ending frame payloads to determine successful download, or have header with number of frames and make sure matches.

14. Stream the content when the user does not have rights to download

15. Hash audio in each frame to two bytes and use to modulate bits because it makes it more difficult to change the audio without detecting this in the header or watermark ID.

16. Choose frames or data within frames randomly, based upon a PN sequence to make it more difficult to change audio without detecting this in the header or watermark ID..

17. Branding the label by presenting the label's logo each time the audio is played or downloaded.

18. Linking back to the retailer where you bought the music for connected-content apps with file sharing, possibly while downloading the content or while playing the content.

19. Automatically generating the ID from the TOC ID and track ID.

Multiply-Watermarked Video

Application 09/597,209 details how different video "objects" within a frame (e.g., as utilized in MPEG4) can be separately watermarked.

As a further extension, consider two different types of watermarking techniques. One type is a "background" watermark that essentially is fixed in reference system relative to the overall frame. It may move as the overall scene moves, or just sit there fixed. The other type of watermark travels with MPEG4 objects.

In the latter system, there can also be a watermark which explicitly moves with an object, but always re-watermarks itself as a function of the global frame reference. In other words, even as an object moves relative to the global frame reference, so too can its watermark signal adapt, so that the overall global watermark is uniform across the frame.

These two systems are not necessarily mutually exclusive. With two watermarks being applied, one level can remain essentially fixed, painting the whole frame, while the other follows individual object patches and may contain object-specific watermarks.

One such approach ties an MPEG4 object locator reference coordinate system into the subliminal grid (calibration signal) detailed in application 09/452,023.

Device Control Watermarks

It is believed that watermarks will first find widespread deployment in audio and video markets as part of copy control system (e.g., the watermark may signal to a compliant consumer device, "Do not Copy," "Copy Once," or "Copy Freely," etc.). Many other applications of watermarking may then follow (e.g., "connected content" applications).

The watermark detection system in the consumer device can be implemented in hardware or software. However, it may be advantageous to have a split arrangement,

e.g., with the copy control watermark being detected by hardware, and the connected content watermark being detected by software.

The circuitry to detect the copy control watermark may be comparatively simple, since the copy control watermark payload is relatively small (e.g., 1-8 bits). Speed is important in this application to assure that useful clips of media are not wrongfully copied. The software to detect the other, added functionality, software, in comparison, can be relatively complex – both to handle a longer watermark payload, and to perform more complex response actions.

In some embodiments, hardware circuitry can detect merely the presence of a watermark, but not decode it. The presence of the watermark can signal something about the media signal (e.g., that it should not be copied, or it is adult content), or may simply trigger the further step of a watermark reading operation (e.g., reading a copy control watermark, or an added functionality watermark). The presence of the watermark can be detected by various means, including detection of the calibration signal disclosed in application 09/452,023, or by sensing some other signal attribute.

Extended payloads have been proposed so as to enable additional functionality (e.g., specifying internet addresses to which consumers can link for additional content or information, specifying the number of times a video can be viewed, specifying the period of time in which an audio selection can be played, specifying database records in which metadata associated with the content (including any of the foregoing information) may be stored, etc.)

As such, watermark decoding is performed by two decoders. A first, hardware, decoder, is used to read a first set of bits (typically associated with copy control functionality). A second, software, decoder, is used to read a second set of payload bits (typically associated with extended functionality that does not involve basic copy control operations).

Typically, although not necessarily, the two watermarks payloads are conveyed by two distinct watermarks, using different watermarking algorithms or different key (noise) data (i.e., they are not simply different bits of a single watermark). The two watermarks may be applied to the content sequentially, or in a single operation.

An advantage to the above-described approach is security. Software is easier to reverse engineer than hardware. A hacker who reverse-engineers a software decoder to interfere with the extended payload, and associated functionality, does not thereby compromise the hardware detector, and the associated copy control functionality. Moreover, if different watermarking algorithms are used, information gleaned in reverse-engineering the extended watermark or its software decoder does not compromise the security of the copy control watermark or its hardware decoder.

This approach also reduces the gate count of the hardware decoder – an important consideration in mass produced consumer electronic devices. Moreover, it permits the same hardware to be employed in a range of different products – products that are differentiated by software-provided functionality.

This approach can be used with both audio and video content. Moreover, it is also applicable to still image content, including conventional graphic files (e.g., JPEG'd photographs) and scanner data corresponding to paper documents (e.g., generated by a photocopier).

Watermarks and Cinema

Watermarking has many uses in the field of Digital Cinema. Some work is being done in this field by the Digital Cinema working group of the Society of Motion Picture and Television Engineers (SMPTE).

In one arrangement, a watermark is dynamically embedded in the video, in the pipeline of data to projector, thus embedding information such as a) what video disc or other media is this (each piece of media may have a unique identifier so that movie distributors can track them) b) what theater the current projector belongs to, and c) what time and date the movie is being shown. Future digital camcorders etc. could have a watermark reader chip in them, and when it detects a watermark in the scene it is filming, the camera could prevent recording. For older camcorders which would not have this hardware, the presence of these unique id's allows authorities to determine at exactly what theater the illegal filming took place. Since many of the pirated movies are taken from the projector booth so as to get a clean line of sight of the film, and to

tap into superior audio, the date and time data could be used to determine who was running that projector when the illegal copy was made.

In another arrangement, watermarking can be effected in the auditorium (e.g., for showtime/location serialization, etc.) by use of a slide with a variable transparency in front of the projector. Desirably, this wouldn't be put in front of the lens, as this is near the conjugate plan of the optical system, and unless the watermark is purely in the Fourier domain, much would be lost. Generally the watermark added signal should be in the focal plane. This is the least expensive approach and easy to change often. These two advantages are important because Digital Cinemas don't want to spend any extra money, especially on content protection that may degrade quality. Furthermore some digital cinema set-ups use a digitally controlled gate in the focal plane of the projector. The local watermark can then simply be an adder to the digital input for the cinema

In some cases, such a slide may be visible because the watermark is not moving or changing. To redress this, the system could use an LCD array or light valve that changes over time. Some property of the watermark would change from frame to frame, perhaps the origin of the grid, perhaps the payload, and thus make the watermark appear as time dependent noise rather than fixed pattern noise.

The watermark can be relatively weak since the ID only need to be detected somewhere in the movie, and watermark signal from multiple frames can be used to aid the detection. Reliable detection once every, e.g., 5 or fifteen minutes, can employ thousands of frames of data (e.g., at 25 frames per second).

On the production and distribution side, of course, a watermark can be applied at any stage of the process –the camera that first captures raw footage, the non-linear editing machine that produces the final editor's cut, the mastering machine that produces distributed content, the transmission system that distributes the final content to the theatres, etc., etc.

In addition to watermarks encoded at time of production and distribution, a further watermark may be added at the theatre, e.g., including time and date of screening.

In cinemas using micro mirror projection devices, the mirrors provide a vehicle to insert subtle changes representing watermark data. For example, each mirror element's reflectivity property can be tailored to as to uniquely serialize each projector.

Of course, the foregoing can also be realized using audio watermarks instead of, or in addition to, video watermarks. In bootlegs made from the projection booth, the sound to the front speakers is usually tapped. If desired, the rear speakers can be provided the same watermark data in opposite phase, causing the watermark to cancel in the auditorium. This may permit a higher energy encoding of the audio watermark than would otherwise be the case.

Finally, cinema screens have holes for sound penetration. By re-arranging the size and/or position of holes, an essentially imperceptible watermark pattern can be formed that serves to identify the particular screen (and cinema).

Watermarks and Digital Object Generation Tools

Document generation tools continue to increase in sophistication and complexity. Adobe offers a variety of such tools, including their InDesign software. Watermarking can advantageously be effected in such systems.

In such environments, a document may be created using a variety of tools – most of which can insert a watermark. One program may use as input the output of one or more other programs (i.e., "compositing").

To better handle watermarking in this environment, a watermarking function (e.g., a PostScript-like command) can be provided in the tools. This function is called with parameters specifying the desired features of the watermark information, e.g., payload, robustness level, masks to be used. At rendering time, such as for on-screen viewing, printing proofs, or ripping the final version, the watermark is actually added as digital data. In such environment, the embedder knows the properties of the rendering device, such as the printer, and appropriately adjust its embedding accordingly. With this concept, watermarks are not lost during composite operations, and watermarks can be embedded in vector (or line) art. Moreover, the color manager at the ripping stage may be the best entity to add the watermark.

This idea likewise extends to video - especially MPEG-4 object video, audio - especially MIDI or MPEG-4 structured audio language, and virtual advertisements.

The use of a PostScript-like function to embed a watermark is further detailed in application 09/629,401.

An alternate method is that no desktop tool has watermarking capability, but instead an on-line watermarking server is available to support common image formats. A variety of tools are enabled to submit images to the server with information regarding the desired parameters of the watermark. The server then returns the image to the application. In this way, the burden of integration is virtually eliminated and the registration and marking take place simultaneously.

The watermarks in content, such as an image, can be used by web page designing software to automatically cause actions to happen, such as automatically add the correct hyperlink for that image into the web page being designed, controlling secure transfer (encryption) of the image in web page. For example, the web authoring tool screens for watermark in images, goes to a central or distributed database and obtains the current link for that image and metadata about that image. The web design tool can place that metadata into a standard form with the image on the web page. In another example, a user drags the image of a house onto web page and web authoring tool screens the watermark, uses it to link to the database, the database returns the pertinent hyperlink to be placed on the web page when that image is clicked and other metadata which is automatically formatted and added to the web page. When watermarked content is dynamically added to web pages at render time, possibly via the use of scripts that determines the correct image or ad to place in the web page at rendering time, the watermark is used to determine the correct hyperlink for the image. Specifically, the web server or dynamic administrator that adds the content screens the watermark and inserts the correct link into the HTML document.

The system can use data embedded in the header, footer or frame of the content, such as a link and description in the header. In this case, the link in the header of the content is added to the HTML of the web page by the web authoring tool. The system can use a watermark, where the watermark is minimally perceptible and includes

around 32-bits of data, and a secondary database lookup to find the desired link and information to automatically be added to the web page during authoring. Finally, the system can use a watermark that contains the information to be added to the web page. For example, the watermark may contain the lyrics of a song, which are added to the HTML web page automatically by the authoring tool when the song is added to the web page. This watermark requires around 30 bits per seconds, which is currently obtainable with non-robust watermarks and will be obtainable with robust watermarks in the future.

The watermark could help the web authoring tool link to a digital asset management (DAM) database, which could provide more information about the content. With the correct template and DAM system, dragging an image into a web authoring tool could cause the whole page to be instantly created.

Intereliant Watermarks

One watermark (or non-watermark meta data) can convey information about a second watermark in the same object. For example, the first watermark can identify a particular algorithm used to encode the second watermark. By decoding the first watermark, information useful in decoding the second watermark is obtained. The first watermark can have a low information content, and thus be relatively inconspicuous. The second can have a much higher information content (e.g., a unique ID identifying the content). By knowing particular information about the second watermark (e.g., the particular encoding algorithm), it can more reliably be decoded without increasing its energy (and visibility).

Text Watermarking

For text watermark, the watermark could add spaces at end of text. The spaces at the end of the line or characters in each line can be used to represent 1's and 0's. For example a line with an even number of characters is a 1 and odd number of characters is 0. In addition, only certain lines could be used, such as lines with specific text. For

example, in watermarking news stories, only the lines with the text "AP wire" is watermarked. The watermark can identify the story or distributor, for forensic tracking.

In addition, the data to be embedded can be modified by a function related to the original text, such as a hash of the text. This way it is difficult to duplicate the watermark.

To provide a comprehensive disclosure without unduly lengthening this specification, the patents and applications cited above are incorporated herein by references.

Having described and illustrated the subject technologies with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while the detailed description focused on digital watermarks to convey auxiliary information with audio and video content, other techniques can be used as well (e.g., VBI, digital fingerprints, header meta data, etc.). Likewise, in embodiments relating to marking of physical objects, other machine-readable data representations can be employed (e.g., bar codes, glyphs, RF IDs, mag stripes, smart card technology, etc.).

The implementation of the functionality described above (including watermark decoding) is straightforward to artisans in the field, and thus not further belabored here. Conventionally, such technology is implemented by suitable software, stored in long term memory (e.g., disk, ROM, etc.), and transferred to temporary memory (e.g., RAM) for execution on an associated CPU. In other implementations, the functionality can be achieved by dedicated hardware, or by a combination of hardware and software. Reprogrammable logic, including FPGAs, can advantageously be employed in certain implementations.

It should be recognized that the particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also contemplated.

In view of the wide variety of embodiments to which the principles and features discussed above can be applied, it should be apparent that the detailed embodiments are

illustrative only and should not be taken as limiting the scope of the invention. Rather, we claim as our invention all such modifications as may come within the scope and spirit of the following claims and equivalents thereof.